**Előházi János**

# VÉDELMI CÉLÚ INFORMATIKAI RENDSZEREK FELADATAI ÉS FENYEGETETTSÉGEI A HÁLÓZATKÖZPONTÚ HADVISELÉSBEN

***Absztrakt***

*This article aims to describe the network based operations, and the role of computer networks within this area. It sums up the possible ways of applying IT systems in network centric warfare, describes the mechanism of a cyber attack, and the possible defense methods against them. Describes the basics of a digital army, C4I systems, and the way how computer agents communicate with each other.*

*As computer systems takes a major role in modern warfare it is more and more important to realize the ways they can be used against an enemy, and it is essential to know how to protect our and our allied systems. Computer systems – just as in business life – are playing a critical role in data storage, information processes and communication (including human communication). A weak point in this infrastructure can lead to compromising the entire computer network, and can cause that our decisions are based on fake data. Computer networks therefore ease life, but require strong attention of data and system protection.*

## Bevezetés

A XX. század utolsó két évtizedében valóságos számítástechnikai forradalom zajlott le. Ez elsősorban annak köszönhető, hogy a számítástechnikai eszközök sebessége drasztikusan növekedett. A sebességnövekedés eredménye lett, hogy a korábban célhardvert igénylő eszközök szerepét a számítógép vette át, egységes platformot képviselve. A korábbi speciális rendszerek feladatait, pedig ezen az új egységes felületen futó programok látták el. A rohamos fejlődés másik mozgatórugója az Internet hálózat széles körű elterjedése. A TCP/IP protokollt használó Internet előnye, hogy független a hálózat fizikai rétegétől, és nem szabja meg a rajta keresztüláramló adatok tulajdonságait sem. Így ugyanazon a hálózaton adat-, hang-, videó- stb. kommunikáció egyaránt megvalósítható.

Ez a két hatás eredményezte, hogy a szokványos kommunikációs csatornák uniformizálódtak, és napjainkban ugyanazon az eszközt használva végezzük a munkánkat, szórakozunk és kommunikálunk.

Az egységes környezet egyrészről költségcsökkentést jelent, mivel ugyanaz a hardver lát el számos feladatot, másrészről a komplikált, multifunkcionális környezet megnehezíti az üzemeltetést, a telepítést és a felügyeletet.

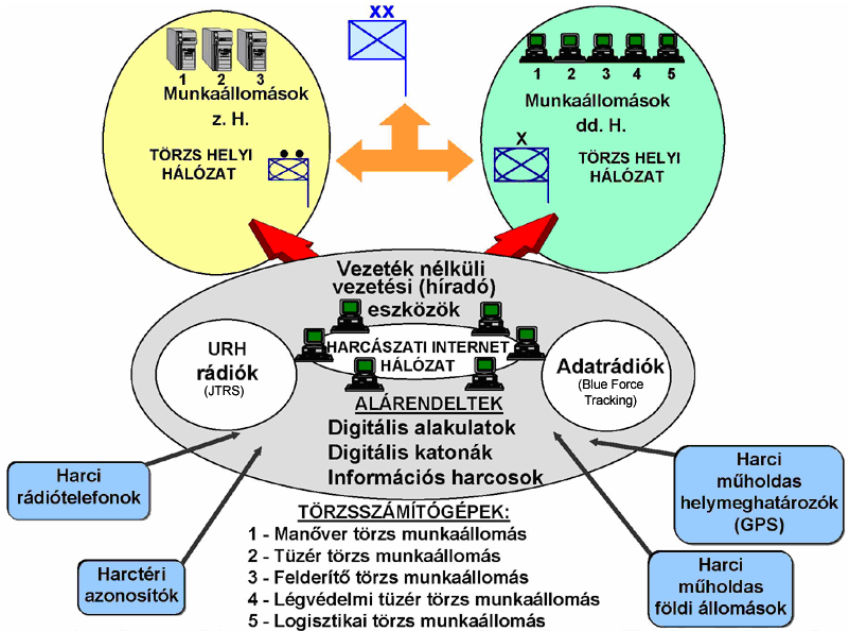
Az Internet előretörése a civil szférában annak katonai alkalmazására is kihatott. A katonai alkalmazásokban is megjelent az uniform platform, és a régi célhardvereket fokozatosan váltják fel a szoftver alapú, multifunkcionális eszközök. A logisztikai és egyéb hasonló területeken a civil szférában régebb óta jelen lévő vállalati irányítási rendszerek mellett, a hadszíntéren is megjelentek a számítógéphálózat-alapú irányítási rendszerek.

## A számítógép és a számítógépes hálózatok a katonai alkalmazásokban

A kibertér előretörésével a hadseregben is paradigmaváltásnak kellett megjelennie, ami képessé teszi a kibertérbeli védekezést és támadást. Ezt a paradigmaváltást új hadügyi forradalom néven említik [1]. Ennek a törekvésnek a lényege, hogy az informatika valamennyi vívmányát, azok védelme érdekében a hadsereg szolgálatába kell állítani. Így szükség van az elektronikai eszközök modernizálására és lecserélésére, illetve az újfajta védekezési technológiához a haderőmodellt is át kell alakítani. A sajátossága ennek a hadügyi forradalomnak, hogy nem zárul le, folyamatosan követi a technológiai fejlődést, és alkalmazkodik az ezek által támasztott új követelményekhez.

### A digitális, hálózat-alapú hadsereg

A digitális, hálózat-alapú hadsereg az informatika valamennyi vívmányát alkalmazza: precíziós fegyverekkel rendelkezik, vezetése integrált harci-hálózati rendszerekre és multimédiás technológiára alapozott, a minőségi mutatók előbbre valóbbak a mennyiségieknél, hatékonysága információ-alapú szemléletének köszönhető, így tudás alapú hadseregnek is nevezhető. Csapásmérő ereje a szemben álló felek aszimmetrikus helyzetéből adódik. Az elsődleges cél az információs fölény megszerzése, mellyel a saját erők, az ellenséget megelőzve tudnak hatékony támadást kivitelezni. Az információ hatékony begyűjtése és tárolása mellett szükséges, hogy azok gyors feldolgozására is képes legyen; rendelkeznie kell olyan felülettel, amelyen minden szükséges információt áttekinthető módon képes ábrázolni, az adott felhasználó igényei szerint. [1]
A digitális hadsereg alakulatai digitalizáltak: a legkorszerűbb informatikai eszközöket felhasználva képesek végrehajtani a globális digitális hadszíntéren információs műveletekkel kombinált hadműveleteket. A digitális hadsereg technikai eszközeinek rendszere a 1. ábrán található.




**1. ábra:**
*Digitális, precíziós, hálózatos hadsereg* [2]

A hadseregben jelenleg alkalmazott hadviselési forma szerint az érzékelő és a csapásmérő képesség egységet alkot. A digitális hadseregre jellemző hálózatközpontú hadviselés az

érzékelő- és a végrehajtó erők közé beiktatja a teljes vezetési-döntéshozó rendszert. Így a felderítési adatokat el kell juttatni a döntéshozókig, majd onnan a feladatokat továbbítani kell a végrehajtó erőkig. Ez a hierarchia az alábbi követelményeket támasztja:

- valós idejű és biztonságos kommunikációt az érzékelők és a döntéshozók között
- az adatok valósidejű továbbítását, feldolgozását, megjelenítését és hatékony felhasználását
- decentralizált adatstruktúrát, amely minden döntéshozó számára biztosítja az adatokhoz való hozzáférést és azok kiértékelését. [1]

**C4I rendszerek**

A C4I betűszó mögött öt angol kifejezés áll:

- Command (vezetés)
- Control (irányítás)
- Communication (híradás)
- Computer
- Intelligence (hírszerzés)

A C4I rendszerek katonai információs rendszerek, a hálózatközpontú hadviselés metodikájának megfelelő komplex vezetési rendszerek. Egységbe foglalják az információgyűjtést, tárolást, feldolgozást, kommunikációt, csapatok vezetését. Biztosítják, hogy a szükséges adatok mindig a megfelelő helyen és időben rendelkezésre álljanak.
A C4I rendszerek feladatai:

- a harctevékenység támogatása a harc minden időszakában;
- biztosítani a csapatok felkészítését, a gördülékeny átmenetet a béke helyzetből a háborús helyzetbe;
- folyamatosan figyelemmel kísérni és értékelni a saját csapatok és az ellenség helyzetét;
- biztosítani az adatok és információk gyűjtését, feldolgozását, továbbítását és elosztását;
- biztosítani a riasztást és a csapatok kiértesítését;
- biztosítani a csapatok követését, irányítását és a tőlük érkező jelentések fogadását;
- támogatni a háborús helyzetből a béke helyzetbe való átmenetet;
- védelmi tevékenységekkel biztosítani az információs rendszer hatékony működését; [3]

**Hálózatközpontú hadviselés**

A hálózatközpontú hadviselés vívmányai segítségével a parancsnok mindig tudja csapatainak pontos tartózkodási helyét, a rendelkezésükre álló lőszert, üzemanyagot és egyéb erőforrásokat. Ismeri a logisztikai információkat, mint az utak állapotát, időjárási helyzetet. Ezek segítségével modellezheti döntéseinek eredményét, előre lejátszva a lehetséges jövőben történéseket.
A hálózatközpontú hadviselés bevezetéséhez három alapvető lépést kell megtenni:

- A meglévő hálózati technológiát hozzá kell igazítani a harci körülményekhez
- A meglévő műveleti eljárásokat hozzá kell igazítani a hálózati rendszerhez
- Újra kell szervezni a klasszikus katonai hierarchiát annak érdekében, hogy a hálózati elképzelések megvalósíthatóak legyenek [5]

A legnagyobb probléma jelen esetben a különböző architektúrák jelenléte. A különböző haderőnemek saját igényüknek megfelelően alakítottak ki vezetési rendszereket, melyek egymással nem, vagy csak részben kompatibilisek. A közös architektúrának platform függetlennek kell lennie. Az amerikai haderőben e közös műveleti környezet az ABCS (Army Battle Command and Control System), melyhez kapcsolódnak a FBCB2 (Force XXI Battle Command Brigade and Below) harcászati szintű rendszerek. [3]

**Információs műveletek**

Az információs műveletek célja az információs fölény elérése és megtartása. Ehhez szükséges a felderítő eszközök, a vezetési folyamat és a végrehajtó erők szoros és gyors együttműködése. Az együttműködés leghatékonyabb megvalósítása számítógépes hálózatok felhasználásával lehetséges, mivel így a rendszerek megosztják erőforrásaikat (ideértve az információt is). Az információs műveletek az információ műveleti biztonságát, az elektronikai hadviselést, a számítógép-hálózati hadviselést, a dezinformálást, valamint az ellenséges információs rendszerek megsemmisítésére kidolgozott technikákat tartalmazza, kiegészítve a pszichológiai műveletekkel, a PR-, a polgári-katonai együttműködési műveletekkel, valamint a nyilvánosság informálását szolgáló tevékenységgel. [1]
Az információs műveletek megvalósításához az alábbi célok elérése szükséges:

- Annak a felismerése, hogy minden egyes katona egyben információforrás.
- Minden egyes katonának és bevetési egységnek érzékelnie, jelentenie és analizálnia kell tudni a saját hadszínterének eseményeit.
- Hálózati környezet, ami integrációt és megjelenítési keretrendszert szolgáltat az egyes katonának minden hírszerzési feladat ellátásában [4]

A hálózatközpontú hadviselés illetve az információs műveletek nagymértékben függenek az információs infrastruktúrától. Ezért annak védelme, illetve az ellenség hasonló rendszereinek működésképtelenné tétele elsődleges fontosságú. Az információs műveletek céljai között így szerepel a szembenálló fél információs rendszerének megfosztása lényeges funkcióitól (pl.: logisztikai irányítás, vezetési ismeretek stb.). Ezek a támadó jellegű műveletek általában az egész ellenséges rendszert érintő degradáló hatás elérésére törekszenek. Ezért az ilyen műveleteket hatás alapú műveleteknek is nevezik. Lényegük, hogy a rendszer egészét figyelembe véve, felismerve az adott támadás közvetlen és közvetett hatásait tervezik meg a támadást, így kihasználva a keletkező hatásláncot, lényegesen átfogóbb romboló eredmény érhető el.
Az információs műveletek célkitűzéseinek másik oldala, a saját rendszerek védelme. Az információs műveletek önmagukban nem elégségesek egy háború megnyerésére, de nélküle az információs korszakban háború nem is nyerhető meg. Tekintettel arra, hogy a fejlett információs társadalmak nagyban függnek a számítógép-hálózatok nyújtotta szolgáltatásoktól, számos ország (pl. USA) igen komolyan veszi az IT infrastruktúrája elleni támadást. [1]

## Infokommunikációs rendszerek

A hálózatközpontú hadviselés intenzív kommunikációs terhet jelent a hadsereg számára. A kommunikáció során továbbított adatok mennyisége jelentősen megnő, és az adatok típusa is sokkal változatosabb.
A hadsereg kommunikációs rendszereiben is végbemegy az a változás, ami a civil szférában: az informatikai hálózatok és a távközlési hálózatok integrálódása. Az integrált hálózatok előnye, hogy az adatok típusától függetlenül ugyanaz az infrastruktúra vehető igénybe.

Hátránya, hogy az integrálódás során, az adattovábbításra kiépített hálózati protokollrendszer és architektúra (TCP/IP) kerül felhasználásra telekommunikációs célokra is, így a kommunikáció csak kompromisszumokkal valósítható meg: az adatkommunikációs rendszerek nincsenek felkészítve adatok típusától függő minőségi követelmények betartására. Az adatátvitel során a bitek maradéktalan átvitele a cél, míg multimédia- és hangalkalmazások során a késleltetés csökkentése a cél, akár adatvesztés árán is. Ez a sajátosság abból fakad, hogy a multimédiás és audió alkalmazások az emberi érzékszervek számára továbbít adatokat. Az emberi agy pedig képes kiegészíteni a hiányzó információt vétel során (pl.: kimaradt szótag, hiányzó képkocka), míg az adatok nagy késleltetése lehetetlenné teszi a feldolgozást. Adatfeldolgozó rendszerek esetében a késleltetés nem okoz problémát a megértésben, de az adatrészletek hiánya lehetetlenné teszi azok feldolgozását. Az internet protokoll nem teszi lehetővé QoS (Quality of Service) szintek definiálását (nincs garantált minőség), csupán un. Best Effort (lehető legjobb) eredmény elérését ígéri.
A katonai infokommunikációs rendszerekkel szemben támasztott követelmények:

- pontos és időszerű adatok begyűjtése
- tudás-alapú rendszerek kialakítása, adatanalízis és tudásadatbázis összekapcsolása, tudásszint horizontális és vertikális irányú kiterjesztése
- adat- és tudás-hozzáférési kör kiszélesítése
- információvédelem [1]

A harctéri infokommunikációs rendszerek alapvetően vezeték nélküli, földi vagy műholdas rádió-adatátvitelen alapuló megoldások.
A rádiós kommunikációs lefedettség hasonlít a civil GSM vagy UMTS rendszerekre: a terület cellákra van osztva (bár a harctéren megmaradnak még a hagyományosnak tekinthető pont-pont kapcsolatok is). Egy-egy cella kommunikációs hozzáférését egy központi állomás biztosítja, mely közvetlen, nagysebességű kapcsolattal csatlakozik a harctéri gerinchálózathoz. A rádióhálózatok maximum 40-50 kilométeres távolság áthidalására képesek, sávszélességük, a hagyományos vezetékes megoldásokkal összehasonlítva nagyságrenddel kisebb. A magas frekvenciatartomány használata miatt a tereptárgyak befolyásolják a lefedettséget: a vevő és az adó között közvetlen láthatóságnak kell fennállnia. A rádiófrekvenciák kiosztása bonyolult feladat, mivel azok interferenciáját meg kell előzni. A rádióadások fokozottan ki vannak téve a lehallgatás és zavarás problémáinak.
A műholdas kommunikációs rendszerek alkalmazása során a műhold játssza az átjátszó szerepet, nem a cella bázisállomása. A tereptárgyak nem okoznak problémát, és a lefedettség gyakorlatilag globális.
Mivel mind a műholdas mind a földi rádiómegoldások felfedezhetősége elég magas, a jövőben az optikai adatátvitel irányában folynak kutatások, elsősorban a lézerfény alapú átvitelek állnak a kutatások középpontjában. [3]

## Alternatív kommunikációs irányok

A rádiós adatátvitelnek megvannak a maga előnyei és hátrányai, mint ahogy az a fent leírtakból körvonalazható (lehallgathatóság és szűk sávszélesség, viszont jól ismert és kompatibilis, olcsó architektúra). A hátrányok kiküszöbölése érdekében alternatív megoldások irányába számos kutatás folyik. A lehallgathatóság és a sávszélesség problémájára nagy valószínűséggel az optikai adatátvitel jelent megoldást. Ebben az esetben, csakúgy, mint a mikrohullámú rendszerek esetében szükséges az adó és a vevő közötti rálátás megléte, viszont a fény tulajdonságai között szerepel, hogy lehallgatásával megváltozik a jel, így az rögtön detektálható. Folynak kutatások a lézeres műholdkapcsolatok fejlesztése terén

is, ahol a földi egységek a föld felett keringő műholdakkal lézeres adatátvitel segítségével teremtenek kapcsolatot. [7]
A lézeres adatátvitel legnagyobb hátránya, hogy olcsóbb megoldások esetén az áthidalható távolság pár kilométer csupán. Az időjárás nagyban befolyásolja a vételi minőséget, ködben, erős esőzésben és minden olyan időjárási környezetben, ami zavarhatja az optikai adatátvitelt kivitelezhetetlen a kapcsolatteremtés. Ezek mellett meg kell oldani, hogy a telepítő antennák kilengéseit követni lehessen mindkét oldalon, különben a lézerfény nem ér célba.
A lézeres megoldások legnagyobb előnye a nagy sávszélesség. Ezek mellett nem elhanyagolható a minimális interferencia, szemben a rádióhullám sávtartományának telítettségével. Az adatátvitel nehezen lehallgatható, mert bármilyen eszközt a sugárnyaláb útjába állítva a kapcsolat megszakad, vagy az átviteli közeg (fény) olyan mértékben módosul, hogy a lehallgatási kísérlet azonnal detektálható. [7]
Mind a rádiós mind a fent vázolt lézeres átvitel infrastruktúrafüggő, így konfliktushelyzetben sérülékeny, illetve védelmük erőket kötnek le. Ezt kiküszöbölendő, egyre inkább terjednek az un. ad-hoc hálózati megoldások: a térségben szereplő kommunikációs eszközök egyúttal reléként is funkcionálnak: a hálózat más szereplőinek adatait is továbbítják a saját adatforgalmuk mellett. Kellő sűrűségű lefedettség esetén (hálózati elemek nagy sűrűsége esetén) ez a megoldás felválthatja a telepített átjátszó állomásokon alapuló rendszereket. Mivel az ilyen hálózatok folyamatosan változnak, és nem biztosított az állandó kapcsolat, a gyakorlatban az ad-hoc hálózatok és az átjátszó állomások módszerét vegyesen alkalmazzák, így megnövelve a bázisállomás által lefedett területet.
Az ad-hoc rendszerek fejlődésének egyik ága a Smart Dust projekt. A miniatürizálás terén elért fejlettséget kihasználva nagyszámú apró adó-vevőket és szenzorokat juttatnak ki a lefedendő területre. A megoldás előnye, hogy egy nagy teljesítményű, könnyen megsemmisíthető rendszer helyett (bázisállomás), számos kisebb teljesítményű kommunikációs eszköz továbbítja a jeleket. A gyakorlatban a smart dust-ot egyelőre még csak időjárási adatok gyűjtésére alkalmazzák, de folynak fejlesztések az adatátvitel terén is. Ebben a megoldásban az ad-hoc hálózat magját a kihelyezett smart-dust mező adja, melyek képesek nagyobb távolságba továbbítani a jeleket egymáson keresztül. Természetesen ezek az apró rendszerek korlátozott erőforrással rendelkeznek, és csak addig használhatóak, amíg rendelkeznek energiával.
A smart-dust eszközök ismert energiaproblémái kapcsán számos kutatás folyik az energiagazdálkodás terén, hogy a rendelkezésre állási időt minél jobban megnöveljék ezekben az eszközökben. Ennek megfelelően teljesen kikapcsolt állapotba kerülnek, amennyiben nincsen feladatuk, illetve léteznek olyan megoldások is, amely során napenergiával működő szemcséket alkalmaznak. Az energiahatékonyság növelése érdekében ezek az eszközök optikai módon kommunikálnak egymással, illetve a bázis-rendszerrel, mivel a rádióhullám alapú megoldásoknál az optikai kommunikáció lényegesen alacsonyabb energiát igényel. [8]

## Információs rendszerek fenyegetettségi formái és védekezési megoldások

Az Internet térnyerésével, és egyre kritikusabb célokra való felhasználásával egyidejűleg annak felhasználásával végrehajtott támadások száma is megsokszorozódott. Azok a felhasználók, akik nem fordítanak elég figyelmet rendszerük védelmére, nemcsak saját maguknak okoznak kárt. A leggyakoribb támadások napjainkban teljesen automatizáltak, és un. zombi-számítógéprendszerek hajtják végre a műveleteket. Ezek a rendszerek az elővigyázatlan felhasználók számítógépeiből állnak, és kapacitásuk egy része alá van rendelve

a támadási funkcióknak. A kiterjedt támadó géppark miatt minden Internetre kapcsolódó rendszert komolyan kell védeni.
Az információs rendszerek elleni támadások a következők szerint kategorizálhatóak:

- illetéktelen adathozzáférés és adatbevitel
- rosszindulatú programmodulok bejuttatása a rendszerbe
- a rosszindulatú programok felhasználásával véghezvitt adatrongálás
- az információs rendszer adatainak megszerzése [1]
- DoS (Denial of Service) vagy DDoS (Distributed Denial of Service) támadások, melyek a rendszer rendelkezésre-állását támadják meg.

Mivel a harctéri rendszerek valamilyen vezeték nélküli adatátvitelt alkalmaznak, fokozottan ki vannak téve az adatátvitel lehallgatásának, illetve a zavarás veszélyének. A vezeték nélküli adatforrások könnyen bemérhetőek, ami fizikai pusztításukat könnyíti meg.

**Számítógép-hálózati hadviselés**

Ahogy a civil szférában úgy a hadseregben is az elsődleges kommunikációs közeg a TCP/IP hálózatok és a WEB alapú megoldások. De miként a civil szférában is veszélyeztetettek az ilyen rendszerek, ugyanúgy a katonai megoldásokat is erősen kell védeni, mivel a civil szférával azonos infrastruktúra (TCP/IP, WWW, e-mail stb.) miatt leegyszerűsödött a katonai rendszerekhez való hozzáférés is. Másfelől az azonos infrastruktúrának köszönhetően egy újfajta hadviselési forma is megjelent, ez pedig a számítógép-hálózati hadviselés. Ezen új hadviselési forma az információs műveleteken belül, együtt más információs támadó és védelmi képességekkel (elektronikai hadviselés, megtévesztés, pszichológiai hadviselés stb.), jelentős mértékben képes biztosítani az információs fölényt a saját erők számára.
Az információs társadalom kialakulása egyúttal azt is jelenti, hogy nagymértékben függünk az infokommunikációs hálózatoktól. A számítógép-hálózati hadviselés egyik célja pedig pontosan a számítógépes hálózatok működésképtelenné tétele.
Az ilyen fajta hadviselési formának két nagy feladata van: egyrészről az ellenség rendszereit kell megbénítani, másrészről a saját rendszerek hatékony védelmét is el kell látni. A támadó-tevékenységek közé tartozik az ellenséges számítógép-hálózatok struktúrájának feltérképezése, ezáltal a gyenge pontjainak a meghatározása. Forgalmuk elemzése alapján megállapítható elhelyezkedésük a forgalmi-hierarchia rendszerben, illetve meghatározhatóak működési sajátosságaik. Az adatáramlás elemzésével megtévesztő információ juttatható a rendszerbe, amellyel elérhető a cél program- és adattartalmának megrongálása is. A védelmi tevékenységek pedig az ellenség ilyen irányú lépéseinek kivédéséből áll. [1]
Elmondható, hogy a nagyhatalmak valamilyen formában mind hadrendbe állították saját számítógép-hálózati hadviselési egységeiket. Hagyományos értelemben a legszervezettebb megoldással az USA rendelkezik. Az USA minden haderőneme rendelkezett a 90-es évek végére informatikai megoldásokon alapuló vezetési rendszerekkel, a kihívás ezek interoperabilitásának megoldása volt. Itt szerepet játszik az is, hogy a NATO szövetségesek jó része nem, vagy csak részben rendelkezik C4I megoldásokkal, melyek szintén különbözhetnek az USA által implementált rendszerektől. Itt legmagasabb a precíziós és robot fegyverek alkalmazása is.
Kína esetében politikai indíttatású a kibertér-beli erős jelenlét. Kína politikai vezetése erősen cenzúrázza a kínai hálózaton megjelenhető tartalmat. Feltételezhető, hogy rendelkeznek azokkal az erőforrásokkal, melyek lehetővé teszik, hogy a teljes országba bejutó online tartalmat szűrjék. Ráadásul Kína rendelkezik talán a legnaprakészebb technológiával is, hiszen a világ szinte valamennyi informatikai gyártója Kínában készítteti el eszközeit, és a

kínai politika része, hogy a gyártási eljárást és a technológiát meg kell osztani a kínai féllel minden esetben.
A legegzotikusabb képet talán Oroszországban találni. A gyenge ellenőrzés és a rossz gazdasági helyzet miatt számos hacker és egyéb számítógépes bűnöző található Oroszországban. Számos (bulvár) hír erősíti meg azt a tényt, hogy Oroszországba, a viszonylag alacsony internet-penetráció ellenére kiterjedt hacker tevékenység folyik; ezek a támadók külföldi megrendelésre több millió kéretlen elektronikus levelet (spam) továbbítanak nap, mint nap, dDoS támadásokat intéznek külföldi infokommunikációs rendszerek ellen. A hetekben zajló észt-orosz politikai konfliktus arra is enged következtetni, hogy az orosz politikai vezetés is kihasználja az ország ilyen célú „eszközeit" (számos észt banknak le kellett tiltania a külföldi hozzáférést rendszereikhez ennek következményeképp).

**Számítógép-hálózati támadások**

Számítógép hálózatok támadásánál meg kell különböztetünk a felderítés és a támadás fogalmát. A felderítés célja a szembenálló fél számítógép-rendszereibe való bejutás, hogy az ott tárolt adatokat és információkat megismerjük, illetve a rendszert feltérképezzük. A támadás célja az információszerzéssel szemben, a károkozás, dezinformáció, rendelkezésre állási képesség megszüntetése vagy drasztikus csökkentése. Mivel a korábban ismertetett harctéri rendszerek egyre elterjedtebbek, illetve mivel – mint manapság mindent – a felderítési és egyéb adatokat számítógéprendszereken tároljuk, a számítógép-hálózati támadások mind a harctevékenység ideje alatt, mind azt megelőzően is hatásosak. Harchelyzetben az operatív működést akadályozza, illetve teszi lehetetlenné, a megelőző időszakban pedig a felkészülést nehezíti. [1]
Illetéktelen adathozzáférés elérhető a rendszer biztonsági réseinek kihasználásával, vagy a rendszer hozzáféréséhez szükséges eszközök illetve tudás megszerzésével. Sok esetben az adatok hozzáférhetőek miközben a hálózaton mozognak. Ez legegyszerűbben vezeték nélküli hálózatokon valósítható meg, mivel a rádióhullámokat egyszerű lehallgatni. Vezetékes rendszerek esetében megoldható a hálózat routereinek útvonalválasztó algoritmusainak olyan módosítása, amely során a forgalom a támadó rendszerein keresztül továbbítható, lehetővé téve azok monitorozását. A hálózat forgalmának titkosítása megoldás lehet a problémára, de minden komoly titkosítási eljárás komoly infrastruktúrát igényel, ami a harctéri rendszereknél nehezen megvalósítható.
A támadás végrehajtható rosszindulatú szoftverek bejuttatásával is az ellenséges rendszerbe. Rosszindulatúnak az a szoftver tekinthető, ami nem az információs rendszer működésének a biztosítása érdekében kerül az információs rendszerbe, melynek tevékenysége az információs vagyon ellen irányul. Az ilyen szoftverek végrehajthatnak pusztítást a szemben álló fél rendszerében, lehetővé teheti a jogosulatlan bejutást a rendszerbe, módosíthatja a tárolt adatokat, illetve továbbíthat bizonyos információkat a támadó számára. Az ilyen programok sajátossága, hogy a felhasználó tudta nélkül végzik tevékenységüket. Leggyakrabban e-mailekkel illetve azonnali üzenetküldő rendszereket használva juttathatóak be, de egyre elterjedtebb, hogy csupán egy weblap megnézésével elérhető településük a célrendszerben. Az ilyen programok általában képesek arra, hogy település után más gépekre is feltöltődjenek. A civil életben az ilyen programok lehetőséget adnak, hogy a számítógép a felhasználó tudta nélkül különböző műveleteket (leggyakrabban elosztott túlterheléses támadást dDOS – Distributed denial of service attack) hajtsanak végre, szenzitív adatokat továbbítsanak a felhasználóról. Eltávolításuk sokszor a rendszer további használhatóságát okozza, így azt újra kell telepíteni, ami jelentős időt igényel és adatvesztést jelent. Az ilyen programok angol elnevezése: malware.

A támadások eredményeképpen, amivel feltétlenül számolni kell, az a saját rendszerek teljesítőképességének csökkenése. Ez egyrészt adódik a támadások ellen fellépő megoldások aktivitásából, illetve a sikeres támadások során, az ellenség céljait támogató feladatok végrehajtásából. Súlyosabb esetben a hálózat használhatatlanná válhat a túlterheléses támadások következtében, adatokat veszthetünk, illetve a számítógépek instabillá válhatnak. Nem elhanyagolható szempont az a veszteség sem, ami az esetleges adatlopással jár: az adat vagy az ellenség kezére kerül, illetve a támadó tetszőlegesen értékesítheti, vagy publikálhatja azokat. [1]
Egyre gyakoribb módszer a mobil eszközök megszerzése, és így a rajtuk tárolt információ eltulajdonítása. Ez jelenti a laptopok, illetve PDA-k illetéktelen kezekbe kerülését. Ennek a módszernek az előnye, hogy a támadónak nem kell bonyolult cyber-műveleteket végrehajtania, illetve nem kell rendelkeznie az azok végrehajtására képes összetett és drága rendszerekkel.

**Számítógép-hálózatok védelme**

A számítógép-hálózatok védelmének fogalma magában foglalja a fent leírt támadási formák elleni védekezést: adatlopás, illetéktelen hozzáférés, rendelkezésre állás lerontásának céljából elkövetett tevékenységek elleni módszerek. Mivel a mindennapi élet és vele együtt a katonai vezetés is egyre nagyobb mértékben függ az információs rendszerektől, azok védelme egyre nagyobb jelentőséggel bír. A védelem megtervezésénél alapvetően két szempont szerint kell eljárni: a védelem maga ne kerüljön többe, mint a védelem tárgya; mindaddig sikeresen ellen kell állni a támadásoknak, amíg a védendő információ és rendszer értékes.
A számítógép-hálózat védelmi megoldásait két nagy csoportra oszthatjuk: aktív és passzív megoldásokra. A passzív módszert alkalmazó műveletek csak akkor reagálnak, ha támadás történik, és az ellen lépnek fel, hogy az adott támadás sikeres legyen (pl: tűzfalak, vírusírtók). Az aktív eljárások a támadó rendszerei ellen az általa is alkalmazott támadásokat hajtja végre. Ide tartozik a megelőző támadás, ellentámadás és az aktív megtévesztés. [1]
A tűzfalak átjárópontot jelentenek a védett és a nyilvános hálózatok között. A védett hálózat irányába és az onnan induló forgalom csak rajtuk keresztül mehet át. Ezt kihasználva képesek az átmenő forgalmat figyelni és megszűrni. Feladatuk, hogy akadályt képezzenek a külső támadással szemben. Két alapvető típusú tűzfal létezik: protokoll alapú és forgalom alapú. A protokoll alapú tűzfalak ismerik az alkalmazás protokollját, és mint proxy szerepelnek a hálózatban. A kapcsolatban lévő felek vele kommunikálnak, és ő osztja szét tovább a forgalmat. Így a vevő fél számára a proxy tűnik küldőnek, a küldő számára pedig a proxy tűnik fogadónak. Az ilyen típusú tűzfalak elég erős védelmet nyújtanak, mivel ismerve a protokollt (alkalmazást) az üzenetek tartalmét képesek megérteni, és így azok alapján is tudnak szűrni. A forgalom alapú tűzfalak arra képesek, hogy bizonyos IP cím-tartományok hálózati hozzáférését szabályozzák, illetve, hogy bizonyos portokat letiltsanak a külső világ számára. Minden alkalmazás egy un. porton várja a kapcsolatokat, letiltva az adott portot, a szolgáltatás kívülről nem elérhető. Így elsősorban nem biztonságos alkalmazásokat, mint a TELNET vagy az FTP szoktak elérhetetlenné tenni a külső hálózatról.
A vírusírtók feladata a kártékony kódok számítógépre településének a megakadályozása. A kártékony kódok szűrése történik egy folyamatosan frissülő adatbázis segítségével, illetve heurisztikus módszerekkel. Az adatbázis esetén bájtkód-azonosságára keres a vírusírtó, míg heurisztikus keresés esetén a program viselkedését veszi alapul. A mai vírusírtók már minden elinduló, letöltendő fájlt átvizsgálnak, mielőtt engednék, hogy a számítógépre kerüljön, de a kártékony kódok folyamatos változásával elengedhetetlen, hogy a vírusadatbázis mindig frissítve legyen. Mivel a vírusok legtöbb esetben e-mailen keresztül jönnek, ezért hatékony megoldás, ha korlátozva van az e-mailben küldhető fájlok típusa (nem tartalmazhatnak olyan

csatolmányt az e-mailek, melyekben lehet vírus, pl.: .exe, .doc stb. fájl). Ebben az esetben egy kevés erőforrást igénylő megoldáshoz jutunk, viszont akadályozhatja a mindennapi munkát, ha túlságosan le van szűkítve a küldhető fájltípusok köre. Erőforrás-igényesebb megoldás, ha az e-mail szerveren is fut vírusírtó, és minden átmenő e-mailt megvizsgál. Ezzel a módszerrel a felhasználói hiba, illetve figyelmetlenség, esetleg nem megfelelő szintű hozzáértésből eredő kár nagymértékben csökkenthető.
A külső behatolók elleni védelem mellett szükséges, hogy a tárolt adatokhoz, csak a megfelelő személy vagy személyek férjenek hozzá. Az egyik legrégebbi megoldás a hozzáférés-szabályozásra a felhasználói név-jelszó párosítás. A modern számítógépek megnövekedett feldolgozó-képességének köszönhetően a csupán ezen alapuló védelem nem elég erős ma már. Léteznek szótárak, melyek tartalmazzák a leggyakrabban használt jelszavakat, és ezek felhasználásával un. szótár alapú támadás indítható, de nem kivitelezhetetlen a un. brute-force támadás sem, amikor minden lehetséges módozatot kipróbálnak a rendszeren, amíg nem találnak egy működőt. A legáltalánosabban használt kiegészítő védelem az un. tokenek és az általuk generált egyszer használható jelszavak. Ezek az eszközök minden percben egy új véletlen számkódot írnak ki a képernyőikre, mely jellemző az adott token-re, de a számsorozatok egymásutánja véletlenszerűnek tűnik. A rendszer képes leellenőrizni, hogy az adott számsor származhat-e a felhasználó tokenjéről, és így képes egy második lépcsős authentikációt beiktatni. A tokenek használatához egy PIN kód is szükséges. Lényegesen magasabb szintű biztonságot jelent a biometrikus azonosítás. Ez az eljárás az emberi test sajátosan egyedi jellemzőit kihasználva azonosítja a személyt. Ez lehet újlenyomat, fül-alak illetve retinakép. Ezek a megoldások általában fel vannak szerelve olyan kiegészítő érzékelőkkel, melyek meg tudják állapítani, hogy a mintát nyújtó forrás életben van-e.
Aktív védelem körébe tartozik a megelőző- és ellentámadás valamit a megtévesztés. Megelőző támadás során szükséges az ellenség ismerete, illetve szükséges az ellenfél rendszerének alapos ismerete, hogy megfelelő hatást érjen el a támadás.
Ellentámadás akkor következik be, ha a behatolást vagy behatolási kísérletet észleltük. Ebben az esetben a bonyolult feladat a támadó vagy támadó rendszer azonosítása. Ezek után olyan ellentevékenységet kell végrehajtani, amely során az aktív támadását a támadó nem tudja folytatni, illetve a jövőben (bizonyos ideig) nem lesz képes újabb támadás kivitelezésére.
Az aktív megtévesztés folyamán egy külön hálózatot hozunk létre, mely a külső támadó számára a támadandó célrendszernek tűnik. Fontos, hogy a támadó biztos legyen benne, hogy az így látott rendszer az eredeti cél. Valamilyen biztonsági rést nyitva hagyva engedjük be a támadót a rendszerbe. Ennek a módszernek a legnagyobb előnye, hogy megfigyelhető az ellenfél támadási módja, és a saját rendszereink biztonságát a szükséges irányba tovább vagyunk képesek fejleszteni. [1]

## Összegzés

Az eddig leírtakból látszódik, hogy az infokommunikációs rendszerek által betöltött szerep ma már más módon nem vagy csak nehezen helyettesíthető. Megjelenésükkel nemcsak az adatfeldolgozás, gyűjtés és tárolás egyszerűsödött, illetve gyorsult fel, hanem egyúttal az elterjedt és széles körben használt infokommunikációs hálózatok egy új platformot is jelentenek, ahol harcokat kell megvívni, illetve saját erőket megvédeni.
A modern számítógépes rendszerek a vezetési rendszerek összetettségének növekedését, a döntés meghozatalának felgyorsulását, az információ szabadabb és gyorsabb áramlását jelentik, de egyúttal nagymértékű használatuk kiszolgáltatottá, és sebezhetővé is tesz

bennünket. Ezért minden egyes szinten tisztában kell lennünk annak korlátaival és gyenge pontjaival, ismernünk kell az infokommunikációs infrastruktúra védelmi megoldásait.
Magyarországról elmondható, hogy erőteljesen fejlődik, és csaknem eléri a nyugati államok által képviselt magas szintű információs társadalmi szintet. Nem létezik bank internetes szolgáltatások nélkül, a hagyományos telefon szerepét átveszik az IP alapú megoldások. Egyre többen használnak széles sávú mobil adatátvitelt (UMTS). Ebből következik, hogy a magyar társadalom egyre inkább függ az informatikai hálózatok által nyújtott szolgáltatásoktól. Magyarország abból a szempontból is különleges helyzetben van, hogy sok olyan cég működik a területén, amely valamilyen globális társaság része (outsourcing cégek). Ezek a vállalkozások a nyugat-európaitól alacsonyabb bérek miatt települtek Magyarországra, hiszen ugyanazt a szakképzett munkaerőt itt olcsóbban kapják meg. Ezek a cégek mindegyike aktív adatforgalmat tart fent a vállalat többi részlegével, mert infrastruktúrájuk nem függetleníthető azoktól, így működésük az IT rendszerektől nagyon nagymértékben függ.
Ennek fényében kijelenthető, hogy Magyarországnak szüksége van olyan erőkre, melyek információs rendszereit képesek megvédeni. Bár jelenleg kijelenthető, hogy szerencsére az alacsony terrorfenyegetettségnek, jelenleg nem célja semmilyen szervezetnek a magyar IT infrastruktúra támadása. Az informatikai rendszerek védelme azonban átfogó, nagy szervezettséget, és alapos tervezést igénylő folyamat, az esetleges támadás ideje alatt hatékony védelem már nem dolgozható ki, ezért biztosan állítható, hogy a fenyegetettség pillanatnyi hiánya nem jelenti azt, hogy nem kell képesnek lennünk az infokommunikációs rendszereink védelmére, hiszen az ország gazdasága nagyon nagymértékben függ a nemzeti infokommunikációs rendszerektől.

## Felhasznált irodalom


[1] Dr. Haig Zsolt, Dr. Várhegyi István – Információs műveletek, ZMNE Egyetemi jegyzet, 2004

[2] Dr. Haig Zsolt – Információs műveletek – Digitális hadsereg, katonai információs rendszerek, előadás, ZMNE

[3] Idegen hadseregek elektronikai rendszerei, multimédiás CD-ROM, ZMNE

[4] Edward T. Bair – Actionable intelligence, ISR Journal 2004 Aug. p46-47

[5] Roger Roberts – The power of the network, ISR Journal 2004 July p46-47

[6] http://www.cab.u-szeged.hu/~bohus/old/valami/03lev/weisz.katalin/ [2007. május 13.] - Lézeres adatátvitel

[7] http://www.globalsecurity.org/space/systems/tsat.htm [2007. május13.] - Transformational SATCOM (TSAT) Transformational Communications Satellite (TSAT) Advanced Wideband System

[8] Sharon Berry – Digital dust sweeps away traditional networking. SIGNAL, March 2001 p53-55

[9] http://www.honvedelem.hu/hirek/kiadvanyok/magyar_honved/euforalthea [2007. május 20.] - Eszes Boldizsár – Vastagh László - EUFOR–ALTHEA